CARRIER FREE TERMINAL AUTHENTICATION SYSTEM USING MAIL BACK SYSTEM

Publication number: JP2002082912

Publication date: 2002-03-22

Inventor: KUMAGAI TAKUYA; MAEDA MARIKO; NAKANO TAKASHI

Applicant: IDS KK

Classification:

- international: ***G06F13/00; G06F21/20; H04L9/32; H04L29/06;*** **G06F13/00; G06F21/20; H04L9/32; H04L29/06;** (IPC1-7): G06F15/00; G06F13/00; H04L9/32

- European: H04L29/06S10C; H04L29/06S8D1

Application number: JP20000285828 20000920

Priority number(s): JP20000285828 20000920; JP20000134500 20000508; JP20000183088 20000619

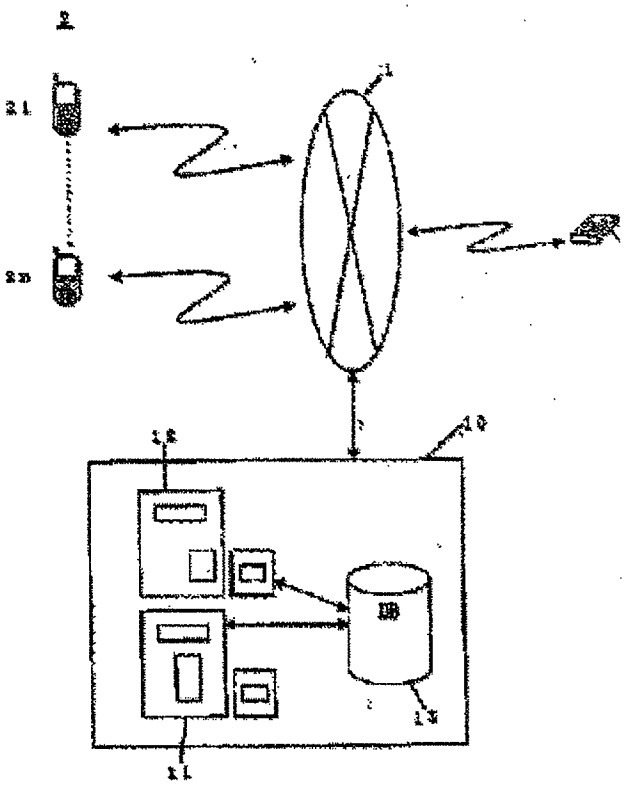
Also published as:

EP1185052 (A2)

US2001039616 (A

Abstract of **JP2002082912**

PROBLEM TO BE SOLVED: To allow a contents provider on a web to provide a carrier free terminal authentication method to a portable terminal using informal site contents. SOLUTION: A parameter to be attached to an URL is made different every time or for every certain fixed time, and made different for every user. In this system, even when all the URL, user ID, and password leak, and another user impersonates a legal user, a new parameter is transmitted to the illegal user, and immediately when a new parameter is transmitted, the previous parameter is invalidated. Then, the new parameter transmitted to the illegal user is not known by the legal user so that the URL to be accessed by the legal user can be attached with the previous parameter. At that time of receiving the access, it is judged that double log-in is performed, and the access from the illegal user and the legal user is invalidated.



(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号
特開2002－82912
（P2002－82912A）
(43)公開日　平成14年３月22日(2002.3.22)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード(参考)
Ｇ０６Ｆ　15/00	３３０	Ｇ０６Ｆ　15/00	３３０Ｃ	５Ｂ０８５
13/00	５１０	13/00	５１０Ｓ	５Ｊ１０４
	６３０		６３０Ａ	
Ｈ０４Ｌ　9/32		Ｈ０４Ｌ　9/00	６７３Ｂ	

審査請求　未請求　請求項の数５　ＯＬ　（全 6 頁）

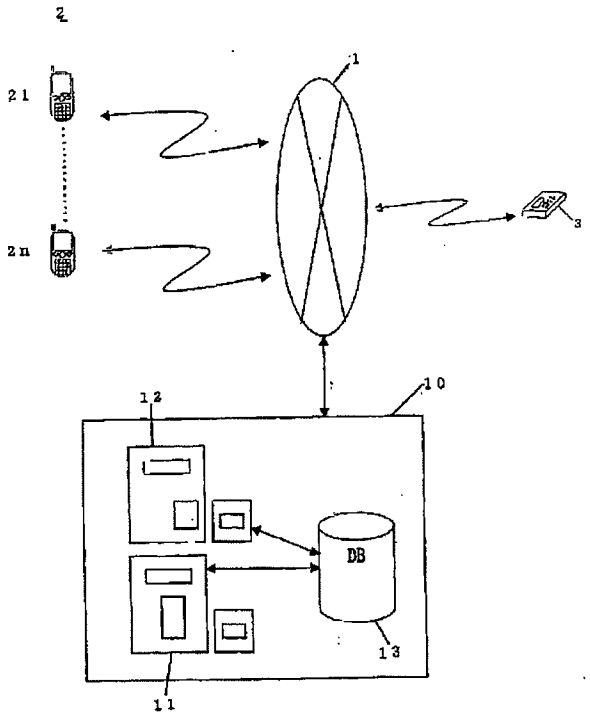
(21)出願番号　特願2000－285828(P2000－285828)
(22)出願日　平成12年９月20日(2000.9.20)
(31)優先権主張番号　特願2000－134500(P2000－134500)
(32)優先日　平成12年５月８日(2000.5.8)
(33)優先権主張国　日本（ＪＰ）
(31)優先権主張番号　特願2000－183088(P2000－183088)
(32)優先日　平成12年６月19日(2000.6.19)
(33)優先権主張国　日本（ＪＰ）

(71)出願人　500205242
株式会社アイディーエス
東京都港区芝２丁目29番11号
(72)発明者　熊谷　卓也
東京都港区芝２丁目29番11号　株式会社アイディーエス内
(72)発明者　前田　真理子
東京都港区芝２丁目29番11号　株式会社アイディーエス内
(74)代理人　100078776
弁理士　安形　雄三　（外２名）

最終頁に続く

(54)【発明の名称】　メールパック方式によるキャリアフリー端末認証システム

(57)【要約】
【課題】本発明においては、ウェブ上でのコンテンツプロバイダーが、非公式のサイトのコンテンツを利用している携帯端末に対して、キャリアフリーの端末認証方法を提供する。
【解決手段】　ＵＲＬについてくるパラメータは１回ごと、若しくは、ある一定時間ごとに異なり、かつ、ユーザ毎に異なるものとする。この方式でＵＲＬ、ユーザＩＤ，パスワードがすべて漏れてしまい、他のユーザが正規ユーザに成りすましたとしても、不正ユーザに新しいパラメータを送り、新しいパラメータを送った瞬間に以前のパラメータは無効とする。正規ユーザは不正ユーザに渡った新しいパラメータはわからないため、正規ユーザがアクセスするＵＲＬは以前のパラメータになる。この時、このアクセスを受けた場合、２重ログインと判断し、不正ユーザと正規ユーザ双方のアクセスを無効とする。



【特許請求の範囲】
【請求項１】　端末及び携帯端末、各種アプリケーションが搭載されたウェブサーバ、ユーザ管理データベース、前記端末及び携帯端末と前記ウェブサーバとの間のセッションを管理するためのサーバミドルウェアから成り、前記ユーザ管理データベースの情報に基づき、前記端末又は携帯端末に送るＵＲＬにパラメータを付与し、前記ウェブサーバから前記端末等に送られるＵＲＬに与えられる前記パラメータは、ユーザ毎、また、ウェブサーバへのアクセス毎に異なるよう設定され、当該ミドルウェアがユーザのアクセスを正規のものと認証した場合、ユーザ専用のホームページを生成すると同時に、メールサーバを起動し、ユーザに前記ユーザ専用ページのＵＲＬが記載されたＥメールを返すことを特徴とするメールバック方式によるキャリアフリー端末認証システム。
【請求項２】前記パラメータは、ある一定期間で変化させることも可能であり、ユーザが、前記ミドルウェアにアクセスする毎に前記パラメータが異なる場合は、一度使用すれば、二度目以降は無効となるようにでき、または一定時間で変化させる場合は、所定の時間が経過すれば、無効となるようにも出来ることを特徴とする請求項１に記載のメールバック方式によるキャリアフリー端末認証システム。
【請求項３】　前記ウェブサーバ上の前記アプリケーションへのアクセス時に、ミドルウェアが正規ユーザのアクセスかどうかを認証し、エラーアクセスであった場合、アプリケーションにエラー情報の種類を送り、特定のエラーの場合には、ユーザがアプリケーションを使用することが可能であることを特徴とする請求項１に記載のメールバック方式によるキャリアフリー端末認証システム。
【請求項４】　前記ＵＲＬのパラメータの過去の履歴をユーザがブラウザの戻るボタンが使用できない環境から複数回使用できる環境までを自由に設定することができることを特徴とする請求項１に記載のメールバック方式によるキャリアフリー端末認証システム。
【請求項５】　前記ミドルウェアはユーザ専用のページを生成し、ユーザはブックマークされた前記ページにアクセスするだけでパラメータが埋め込まれた前記ＵＲＬをＥメールで受信することが可能であることを特徴とする請求項１に記載のメールバック方式によるキャリアフリー端末認証システム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、インターネットサーバにアクセスする端末を限定する為の端末固有の情報を利用せずに、ウェブ上でのコンテンツプロバイダーが、キャリアからの認証情報を利用することなしに端末の認証及びセキュリティの保持を可能とするメールバック方式によるキャリアフリー端末認証システムに関するものである。
【０００２】
【従来の技術】一般的に発生するセキュリティ問題において、端末認証方法として、ユーザＩＤやパスワード（ＰＷ）、更にユーザ専用のホームページを生成する等して、端末情報を管理する仕組みが考えられてきた。
従来の方法として、まず、最も低いレベルのユーザ認証方法は、ユーザ専用ページを作り、そこにアクセスしてきた人だけを正規ユーザとして認定する方法がある（方式Ａ）。これはブックマークに専用ページのＵＲＬ（Ｕniform Resource Locator ）を登録するだけでユーザは常に自分専用のページにワンアクションで入れることから、手軽に使える方法ではあるが、通信をモニターするとすぐ破られてしまう。
【０００３】次にユーザ専用ページを作り、さらにユーザＩＤとパスワードで保護する方法がある（方式Ｂ）。しかし、通信をモニターしたり、正規ユーザが悪意を持ってＵＲＬ、ユーザＩＤ、パスワードの全ての情報を第３者に教えることが起こり得るので、この方法では安全性がない。
【０００４】高い安全性が確保出来る方式として、ユーザ専用ホームページからユーザＩＤとパスワードを入力した上でサーバにメールバックを申込み、サーバから返ってくるＥメールに、１回毎に異なるパラメータが付与されたＵＲＬを埋め込む方法がある（方式Ｃ）。この方式では、Ｅメールは正規契約端末にしか送られないため、たとえ他の端末からメールバックを申込んだとしても、Ｅメールは他の端末には届かないため、正規契約端末だけが、その次のステップに進むことが出来る。
【０００５】
【発明が解決しようとする課題】ウェブ上でアプリケーションを提供するプロバイダーは、そのコンテンツを利用する端末を認証し、その使用料として課金を行ないたい。しかしながら、特定のキャリアにおいて、例えばｉモードでは、ＮＴＴドコモの公式サイトに入っていないサイトを利用した携帯端末の固有情報が利用できないので、ＮＴＴの公式サイト以外のアプリケーションコンテンツは、このＮＴＴドコモの情報を用いて端末認証を行なうことができず、従って、課金処理ができないという問題点があった。また、認証情報は複数のキャリア、例えばＮＴＴドコモ、ＫＤＤＩ、Ｊ－フォン等、の携帯端末等を利用して、送られてくるため、認証サーバはそれぞれのキャリアと認証情報をやり取りする必要があった。特に、国をまたがり、広い地域にサービスを提供しようとする場合に認証の実施が困難であった。
【０００６】認証の安全性を確保するにあたり、以下の４つのケースの問題に関して、いずれの問題が発生した場合においても安全性が確保でき、かつ安全性の要求度合いによって認証程度を設定可能な認証システムを提供

することを課題としている。
【０００７】第１番目は、共通のページに対しパスワードで閲覧を許可するケースにおいて、ユーザＩＤとパスワードが漏れてしまった場合である。これは既にインターネット上でユーザＩＤとパスワードを取引するための市場があることから、一般的に発生するセキュリティ問題である。
【０００８】第２番目は、ユーザ専用ＵＲＬからなる専用ページを作って、他人のログインを防ぐ仕組みの場合に、そのＵＲＬそのものが漏れてしまった場合である。インターネット上ではＵＲＬは一般に暗号化等の処理をされずにバケツリレーのようにサーバ間を行き来する場合があるため、第３者が通信状況をモニターすることで、ユーザ専用ＵＲＬを知ることは容易である。
【０００９】第３番目は、第２番目と同じく、ユーザ専用ホームページを作って、さらにユーザＩＤとパスワードで保護しているにも拘わらず、そのＵＲＬとユーザＩＤ及びパスワードが漏れてしまった場合である。これは、例えば、悪意をもった正式ユーザが、友人同士でそのサービスを共有するために、全ての情報（ＵＲＬ，ユーザＩＤ，パスワード）を公開した場合に発生する。
【００１０】そこで本発明の目的は、ウェブ上でのコンテンツプロバイダーが、サイトの属性によらない、すなわちキャリアフリーの端末の認証方法と同時にシステムのセキュリティを提供することを課題としている。また、コンテンツによってはセキュリティの軽重を考慮し、認証方法の程度（レベル）の設定が可能であるようなメールバック方式によるキャリアフリー端末認証システムを提供することである。
【００１１】認証方法の設定において以下の課題がある。
【００１２】正規ユーザであって、ログインにタイムアウトエラーを起こしても１回だけは情報を提供するなど、ログインエラーの種類によっては、情報提供ができるような設定が可能なシステムを構築する。
【００１３】メールバック方式によるキャリアフリー端末認証システムでは、パラメータは基本的に使い捨てのため、ブラウザの戻るボタンを使用すると不都合が生じる。即ち、戻ることが不可能になる。そこで、ユーザの利便性を考慮して、ブラウザの戻るボタンを使用できない状態から複数回使用できる状態にまで設定可能な機能を提供する。
【００１４】メールバック方式によるキャリアフリー端末認証システムでは、ユーザはログインするたびに本人のＩＤとパスワードを携帯端末のキーボードから入力する必要がある。しかし、携帯端末から毎回ＩＤとパスワードを入力することは煩雑でもあるので、ユーザがブックマークした専用ページにアクセスするだけで、パラメータが埋め込まれたＵＲＬを通知するＥメールが届く仕組みを提供する。ただし、万が一、このブックマークされたＵＲＬが漏れて他人がその専用ページにアクセスしたとしても、セキュリティが確保できるメールバック方式によるキャリアフリー端末認証システムを提供する。
【００１５】
【課題を解決するための手段】本発明は、メールバック方式によるキャリアフリー端末認証システムに関する。本発明の上記目的は、ＵＲＬについてくるパラメータを１回ごと、若しくは、ある一定時間ごとに変化させ、かつ、ユーザ毎に異なるようにし、更に、万が一、ＵＲＬ，ユーザＩＤ，パスワードが全て漏れたとしても、その情報はその時、若しくは一定時間だけにしか使用できない様に設定することによって達成される。
【００１６】この方式でＵＲＬ、ユーザＩＤ，パスワードがすべて漏れてしまい、他のユーザが正規ユーザに成りすましたとしても、本発明の認証システムにより不正ユーザのパラメータと正規ユーザのパラメータを比較することで不正アクセスの発生を検知できる。
【００１７】請求項１は、この認証の仕組みを述べたものである。ミドルウェアは、携帯端末からユーザ名とパスワードを取得し、事前に登録された情報に照合して、正規ユーザと認めた場合、専用のホームページを生成する。
【００１８】専用のホームページアドレスにはＵＲＬとユーザ名及びシークエンス番号の情報が含まれている。ミドルウェアは上記専用ページを生成すると同時にメールサーバを起動し、事前に登録された当該ユーザのＥメールアドレスにＥメールを送信する。Ｅメールには上記専用ページのＵＲＬが記述されている。ユーザはＥメールを受け取り、Ｅメールを開き、上記専用ページのＵＲＬをクリックする。
【００１９】請求項２は、パラメータの変化について述べたものである。ＵＲＬをクリックすることにより、端末のブラウザが立ち上がり、ミドルウェアにアクセスを行なう。ミドルウェアは端末からのアクセスを受け取るとその中に記述されたユーザ名とシークエンスナンバーを判定し、ウェブサーバへのアクセスを許可する。アクセスを許可されたページをミドルウェアは受け取り、次のシークエンスナンバーを埋め込む。一度使用されたシークエンスナンバーはその後無効となる。シークエンスナンバーは類推しやすい番号ではなく、例えば、２Ａ１３と言った、アルファベットと番号を組み合わせたランダムなものとする。
【００２０】従って不正ユーザがＵＲＬをモニターして不正にアクセスした場合、本発明の認証システムは、２重ログインと判断し、不正ユーザと正規ユーザ双方のアクセスを無効とすることが可能になる。
【００２１】正規のユーザは自分のアクセスが無効となった場合、再度メールバックを申込み、新規のパラメータを受け取る。不正ユーザはメールバックを受け取ることが出来ないため、その後は正規ユーザだけがサービス

を受けることが可能となる。

【００２２】請求項３では、ミドルウェアからウェブサーバ上のアプリケーションにステータスコードを送り、正規ユーザからのアクセスかどうかを認証する。このステータスコードは、２値パラメータ、０及び１からなり、０を正規アクセス、１をエラーアクセスとする。エラーの場合、更にステータス詳細コードがアプリケーションに送信される。このステータス詳細コードは、番号が割り振られたエラーの種類をパラメータとし、これらの番号値をパラメータの値としてとる。従って、エラーの種類によっては、アプリケーション情報を提供するかどうかの判断をアプリケーショの管理者が設定可能となる。

【００２３】請求項４では、ブラウザのキャッシュと呼ばれる記憶の中に過去のページ情報を蓄え、ページ情報に埋め込まれている過去０回よりＮ回までのシークエンスナンバーまでは有効とするといった設定が自由にできるような仕組みを取り入れる。だたし、０回を設定すれば、その際はセキュリティを高めるため、戻るボタンは一切使用できなくなる。

【００２４】請求項５では、ユーザがブックマークした専用ページにアクセスするだけで、パラメータが埋め込まれたＵＲＬを通知するＥメールが届く仕組みを提供する。もし、他人がその専用ページにアクセスしたとしても、正規ユーザによって登録されたＥメールアドレスにユーザＩＤとシーケンスナンバーが入ったＵＲＬを送信するので、パラメータが埋め込まれたＵＲＬは正規のユーザにのみ送信される。従ってこの場合はセキュリティが確保できる。但し、この仕組みでは、端末を紛失して、端末そのものが他人の手に渡ったときにはセキュリティが守られないので、あくまでこのブックマークの仕組みは使い勝手とセキュリティのトレードオフとなる。

【００２５】上述の説明からわかるように、請求項３及び請求項４では、ユーザが各自必要とするセキュリティレベルを選択的に設定することが可能である手段に関するものである。

【００２６】

【発明の実施の形態】本発明では、携帯電話等の携帯端末の端末固有の情報、例えばシリアルナンバー等に類する情報を利用せず、ＭＣＦＳＳ(Mobile Carrier Free Security System)と称されるミドルウェアを利用して、従来の問題を解決している。

【００２７】以下、本発明の実施の形態を図面に基づいて詳細に説明する。

【００２８】図１は本発明の基本概念を示しており、インターネット１にはｉモード機能を有する携帯電話及び他キャリアのインターネット接続が可能な携帯電話２（２１～２ｎ）や携帯端末３が接続されており、インターネット１には更にウェブサイト１０が接続されている。携帯端末２及び３は、各ユーザに対して個別に付与されたＥメールアドレスを有しており、ウェブサイト１０は認証ミドルウェアを備えたウェブサーバ１１及びメールサーバ１２を具備しており、ウェブサーバ１１及びメールサーバ１２は各種データベース１３を持っている。

【００２９】この様な構成において、認証システムの手続は図２に示すフローに従って行われる。まず、サイトサービスの利用者（ユーザ）は、携帯端末２にて、サイトの新規登録画面を開き、氏名等の属性、ＩＤ／パスワード、自分の携帯端末のＥメールアドレスを入力する（ステップＳ１）。この入力がサーバを経由して、ユーザの入力情報はウェブサイトでユーザＤＢ（データベース）に登録される（ステップＳ２）。

【００３０】次に、携帯端末からユーザがウェブブラウザでログイン画面を開き（ステップＳ３）、ログイン画面から自分のユーザＩＤ／パスワードを入力する（ステップＳ４）。その後、サーバではユーザＩＤ／パスワードを照合し、正規ユーザの場合は専用ページを生成し（ステップＳ５）、サーバは専用ページのＵＲＬを登録されているユーザのメールアドレスに送る（ステップＳ６）。このメールをユーザが携帯端末で受け取り（ステップＳ７）、メールを開きＵＲＬをクリックするとウェブブラウザが開きサーバにアクセスが発生する（ステップＳ８）。サーバはこのアクセスされたＵＲＬが正しいかどうかを照合し（ステップＳ９）、アクセスを実行したユーザが正規ユーザとして認証できればディレクトリにアクセスを許可する（ステップＳ１０）と同時にアクセスが許可されたウェブページには次のシークエンスナンバーを埋め込む（ステップＳ１１）。ユーザはシークエンスナンバーが埋め込まれているＵＲＬが記述されたリンクボタンをクリックする（ステップＳ１２）。その後、新たなアクセスによるＵＲＬが正しいかどうかをチェックするため、ステップＳ９へ戻る。

【００３１】ここで、ステップＳ５におけるＵＲＬの書式の１例として、http://www.ids.co.jp/members?UN=kuma&SN=2A13等となっている。ＵＮはユーザ名を、ＳＮはシークエンスナンバーを表わしている。シークエンスナンバーは、アクセスの度に変化し、サーバが自動的に生成する。ユーザ名はユーザ毎に一定である。

【００３２】次に、ミドルウェアからウェブサーバ上のアプリケーションに送られるステータスコード及びステータス詳細コードの例を説明する。

【００３３】ミドルウェアからアプリケーションに送る情報の例として次のものを考える。

http://www.my89.com/members?ID=kuma&SC=1&DT=100

ここで　http://www.my89.com/members　はユーザがアクセスしようとしているＵＲＬであり、ID=kuma　はユーザ固有のＩＤである。SC=1　はステータスコードと呼ばれるパラメータで、１はエラーを示し、０は正規アクセスを示す。DT=100　はステータス詳細コードと呼ばれ

るパラメータで、その例として、
DT=100　はシークエンスナンバーが正しくない、
DT=101　は登録されていないＩＤからのアクセス、
DT=102　は同一ユーザによる２重ログイン、
DT=103　はログインに３回続けて失敗、
DT=104　はタイムアウト、
というようなものが考えられる。アプリケーションはこのステータスコード及びステータス詳細コードを受け取り、例えばタイムアウトエラーであっても、１回だけは情報を提供することを許す、などとエラーの種類によって情報の提供を判断することが可能になる。

【００３４】

【発明の効果】本発明は、以上に説明したようなものであるから、以下に記載される効果を奏する。特定の通信会社の公式あるいは非公式のサイトのコンテンツによらず、携帯端末等の認証が可能となる。すなわちキャリアフリーの認証が可能となる。

【００３５】また、この方式では、ユーザＩＤとパスワードを入力しないとメールバックを申込めないため、例え端末が第３者に渡ったとしても、ユーザのシステムの設定環境によっては、それだけでは端末から正規ユーザとして次の処理に進むことは不可能である。即ち、ユーザが要求するセキュリティの度合いに応じて、そのレベルが段階的に設定可能となる。また、ウェブアプリケーション管理者は、ユーザの特定のアクセスエラーに対してユーザがアプリケーションを使用できるよう設定可能となる。

【図面の簡単な説明】

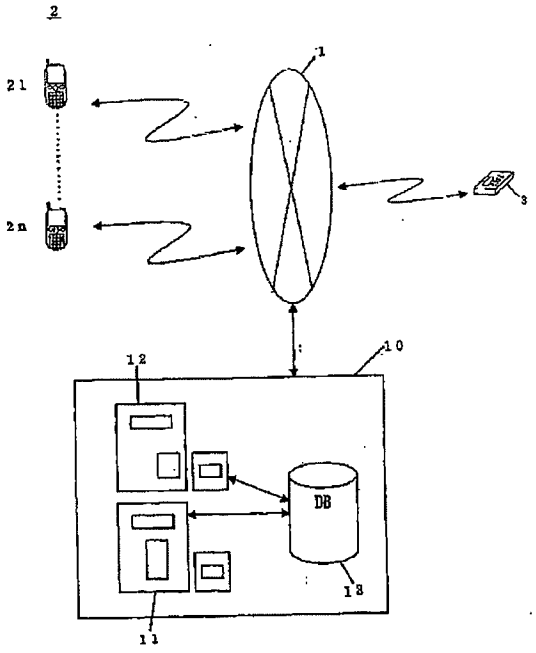
【図１】ウェブサイトの詳細を示すブロック図である。

【図２】認証システムのプロセスを示すフローチャートである。

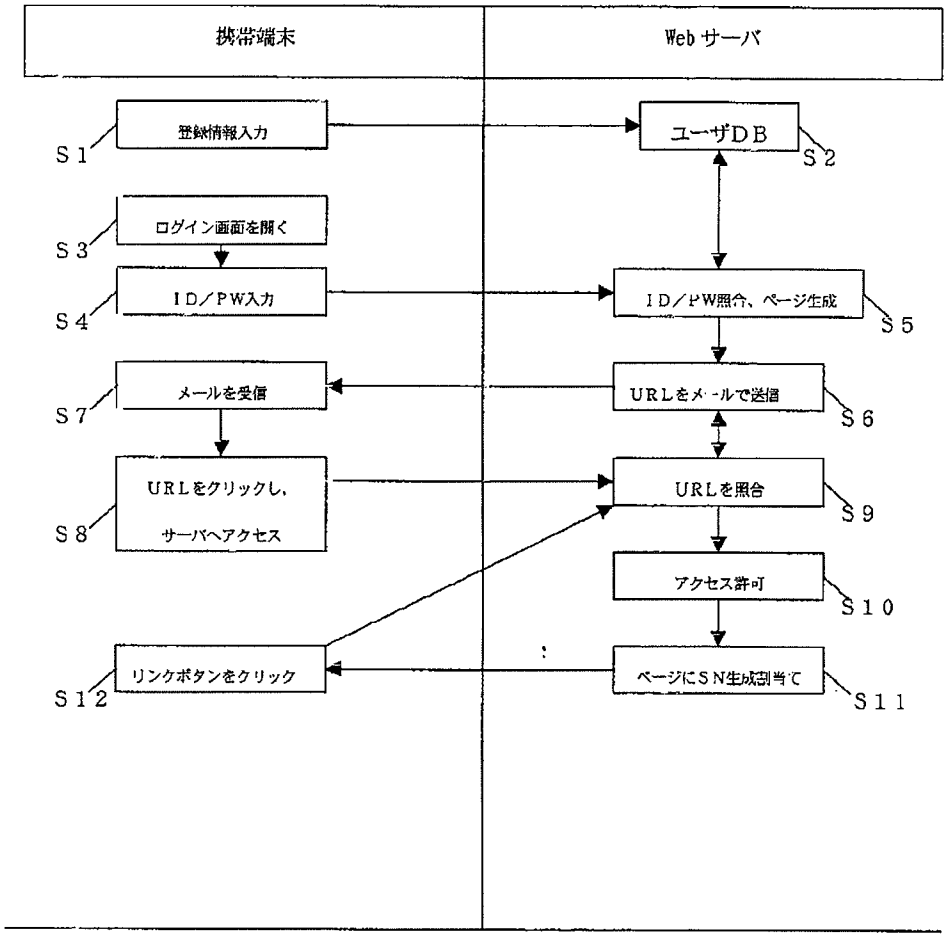
【符号の説明】

1	インターネット
2	携帯電話
3	携帯端末
10	ウェブサイト
11	ウェブサーバ
12	メールサーバ
13	データベース

【図１】



【図2】



フロントページの続き

(72)発明者　中野　貴志
東京都港区芝２丁目29番11号　株式会社アイディーエス内

Ｆターム(参考)　5B085 AA01 AE00 AE06 BE01
5J104 AA07 KA02 KA06 KA21 NA01
PA08 PA11